National Security Agency/Central Support Service

INFORMATION ASSURANCE DIRECTORATE

CGS Acquisition Capability

Version 1.1.1

The Acquisition Capability provides supply chain risk management by determining an appropriate risk management approach for individual acquisitions of products and services. The Acquisition Capability provides research and analysis of suppliers and products and provides that information to the Risk Analysis Capability to make a risk decision regarding whether risks associated with a product or service can be properly managed by the Enterprise.

07/30/2012

CGS Acquisition Capability
Version 1.1.1

Table of Contents

CGS Acquisition Capability

Version 1.1.1

1   Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1

2   Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

The Acquisition Capability provides supply chain risk management by determining an appropriate risk management approach for individual acquisitions of products and services. The Acquisition Capability provides research and analysis of suppliers and products and provides that information to the Risk Analysis Capability to make a risk decision regarding whether risks associated with a product or service can be properly managed by the Enterprise. These measures provide assurance against products having intentional security flaws, supplier personnel posing unknown vulnerabilities, or other risks that may be unacceptable to the Enterprise.

3   Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of "good enough" when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

The Acquisition Capability mitigates security risks associated with Enterprise acquisitions. The scope of the Acquisition Capability spans all purchases, including hardware, software, services (e.g., people and maintenance), and products not related to information technology (IT). Off-the-shelf purchases (e.g., purchases in which an individual walks into a retailer and buys a product off the shelf) and purchases made through the General Services Administration (GSA) shall follow the conditions, procedures, and processes as defined by the Acquisition Capability.

The Acquisition Capability works with the Risk Analysis Capability to determine the security risk level (e.g., low, medium, or high) associated with each proposed acquisition. Many factors contribute to the risk of an acquisition, including the supplier location; supplier political or partner affiliations; clearance level of the supplier, employees, and solution; and the proposed infrastructure location of the products and/or services being procured. For example, purchasing products from an international vendor who has foreign ownership and interests has a higher risk level than purchasing products from a

domestically owned and operated supplier. Suppliers can include contractors, vendors, resellers, distributors, and other service providers. The Acquisition Capability considers the supplier and how the product is going to be used in the Enterprise environment. Suppliers shall be vetted to ensure that they meet the Enterprise assurance requirements. If the supplier is a value-added reseller, the Acquisition Capability requires that the Enterprise determine the value being added to the product and verify that the value-added reseller is not implementing anything malicious or anything that may degrade the product's ability to effectively implement security functions. This determination is made by the Vulnerability Assessment Capability. Third-party suppliers who are not value-added resellers shall never touch a product between the time the original supplier produces it and the purchasing Enterprise receives it.

The Acquisition Capability processes shall conform to security practices as established by the IA Policies, Procedures, and Standards Capability. In implementing consistent supply chain risk management, the Acquisition Capability shall take into account the policies that govern where the product will be implemented. When possible, the Acquisition Capability shall require that suppliers follow the IA Policies, Procedures, and Standards set forth by the Enterprise, which shall require the IA Policies, Procedures, and Standards Capability to have an open communications channel with some of the Enterprise's suppliers. Suppliers following the IA Policies, Procedures, and Standards will reduce the level of risk associated with the supplier and its products.

The Acquisition Capability shall evaluate the background of personnel performing development activities and business processes on products. Personnel Security will issue security clearances to these personnel, where appropriate. The Acquisition Capability shall require that certain products or services be worked on only by individuals who hold a certain security clearance.

Once the risk level has been identified, the Acquisition Capability works with Risk Mitigation to develop a set of mitigation steps that shall be taken to reduce to an acceptable level the risk associated with the proposed acquisition. All acquisitions shall have an associated mitigation plan. Sometimes this plan is simple and can be automatically generated. If not, the plan is decided upon by analysts who will make a final decision. Regardless of the proposed acquisition's risk level, there shall be a mitigation plan for all acquisitions. If the mitigations are implemented, the acquisition will be approved. Free and open source software (FOSS) like any other product shall be accounted for within the Acquisition Capability. Because virtually anyone can contribute to

open source projects, FOSS is almost always defined as a high-risk product by Risk Analysis and so shall be mitigated accordingly.

As part of the Acquisition Capability, a copy of a product's risk assessment report shall be shared with the appropriate information assurance (IA) management personnel for each acquisition that is proposed. If the acquisition request involves removable media or requires the Enterprise to develop a test plan, the responsible IA manager shall approve the requested acquisition prior to procurement.

The Acquisition Capability shall maintain system and network documentation in accordance with Enterprise policy. Whenever the Acquisition Capability approves an acquisition request and a product or service is procured, all of the appropriate system and network documentation shall be updated to reflect the procurement.

External contracts that include IA shall be in compliance with IA standards as a required performance element. When dealing with commercial contracts and commercial off-the-shelf (COTS) products, the Enterprise may have a limited amount of control over the product or supplier, such as with Enterprise license agreements. In this case, as part of the Acquisition Capability, the product shall be vetted and reviewed by the Vulnerability Assessment Capability prior to procurement. Once purchased, the product shall be further tested by Vulnerability Assessment for unexpected behavior and security, prior to being placed in the operational environment. When government off-the-shelf (GOTS) product or service providers can implement IA within the contract, the Enterprise shall include provisions for the foreign procurement of product components and the development of anonymity plans. Anonymity plans dictate if, when, and how a developer shall disclose who they are developing products for without having prior approval.

The Acquisition Capability shall include input from Enterprise information security personnel throughout all of its processes. Once products are supplied, they shall be preconfigured for security; the contracting process to procure the products needs to ensure that acquisition security cannot be circumvented. If it has been determined that services will be outsourced, security consideration needs to be given to the products and processes that will be employed. For example, if a contractor Organization is acquiring products from a third-party supplier on behalf of the Enterprise, the products still shall go through the acquisitions approval process.

The Acquisition Capability shall establish a comprehensive information security strategy to mitigate risks from the supply chain. Some of the components of this strategy include:

- Know the provenance of the IT products and services provided by suppliers.
- Require transparency in the product design and development processes employed by suppliers. This shall be balanced against federal acquisition regulations, which require simplified acquisition procedures.
- Minimize the time between decisions to purchase products or services and the actual delivery date of the products or services. This will reduce windows of opportunity for malicious activity by adversaries. This may not always be possible when dealing with vendors of COTS solutions because the availability of their products may be dictated by market conditions.
- Use standard configurations of products and systems to reduce the probability of malicious code insertion.
- Protect purchasing information, including the buyer's identity.
- Ensure approved distribution processes for products and services. This may be more difficult to achieve with COTS products than with GOTS products because the development of GOTS products can usually be more controlled. For this reason, the Enterprise may establish a policy that prefers purchasing GOTS products over COTS ones.
- Use products that come with manufacturer-supplied unique identifiers, when possible (i.e., serial numbers).
- Use products that have been through an appropriate level of testing and certification, where applicable, such that they are approved for use in the Enterprise. The purchase of such products shall follow Enterprise policy. To facilitate interoperability, Enterprise policy shall define a baseline of products that can be used within the Enterprise. These baseline products shall be selected through a process that includes input from IA personnel. When possible and applicable for the environment, products shall be selected from this baseline list of products. Acquisitions outside of the designated baseline shall be considered on a case-by-case basis, with final approval from the appropriate Enterprise authority.

4 Environment Pre-Conditions
The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.
1. IA goals, strategies, and the business needs have been defined.
2. There is an approved acquisition process.

3. New IT components are tested and visually examined before being placed into the Enterprise.
4. A Risk Management process has been defined and implemented.

5   Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability takes the necessary steps during acquisition to ensure the product or service is in full compliance with applicable IA policies.
2. All outsourced products and services are purchased only through approved suppliers.

6   Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

The Organization will use processes for acquisition to ensure that all new systems and components are accounted for and assessed from a risk perspective throughout the lifecycle. This includes the maintenance of software and hardware components and equipment. The enablers for maintenance functions include the contracts for the technical personnel and services required to keep the systems functioning. Some of the individual functions used to track products across their lifecycle are handled by other Capabilities, including Software Inventory, Hardware Device Inventory, Operations and Maintenance, Configuration Management, Risk Mitigation, and Risk Analysis (see Capability Interrelationships).

The Organization will understand the supply chain risk to mitigate potential use of fraudulent, counterfeit, pirated, unlicensed, or compromised material. The Organization will require its suppliers to do the same, where possible. Ensuring supply chain and software assurance will promote integrity, security, and reliability in hardware and software code development. This includes processes and procedures that diminish the possibilities of erroneous code, malicious code, or trap doors that could be introduced

during development. In general, these processes and procedures will target the following goals:

- Trustworthiness–Ensure that no known exploitable vulnerabilities exist, either maliciously or unintentionally inserted, and that materials are what they claim to be without counterfeit, piracy, or violation of intellectual property rights
- Predictable Execution–Provide justifiable confidence that hardware and software, when executed, function as intended
- Conformance–Provide a planned and systematic set of multidisciplinary activities that ensure hardware and software processes and products conform to IA Policies, Procedures, and Standards.

Toward these goals, the Organization will ensure that acquisition managers and information security managers factor in risks posed by the supply chain as part of their risk mitigation efforts including:

- Information on suppliers' process capabilities (business practices) will be used to determine security risks posed by the suppliers' products and services to the acquisition project and to the operations enabled by the system.
- Information about evaluated products will be made available and reviewed, along with responsive provisions for discovering exploitable vulnerabilities, and products in use will be securely configured.

The Organization will develop IA guidelines that will be followed when establishing contracts with outside Organizations. Contractors will adhere to all of the Organization's established IA Policies, Procedures, and Standards, and compliance with them will be used as a measure of the contractor's performance. If a contractor is to build a product for the Organization, that product will still go through the acquisition approval process and the source of its components will be traced back to the location of origin. All products also will be tested prior to their deployment to operational networks, when possible.

The Organization will use an already developed acquisition process for products and services that reflects its particular functional needs based on the environment it operates in and its mission needs. What follows is an example of how this process will operate. The requester will submit an acquisition request using an automated mechanism. This acquisition request is a request for a risk assessment for the product or service in questions, not a request for funding. The request will immediately be placed into either a low-risk or unknown-risk category. Low-risk requests include a specific and limited set of products for which there are predetermined mitigations. Low-risk requests include items

such as cables and connectors. When a low-risk request is submitted, the requester will immediately receive a list of required mitigations.

Requests that are not immediately identified as being low risk will go to analysis to determine the appropriate risk categorization. This analysis will be conducted by the combined efforts of the Acquisition Capability and Risk Analysis Capability. Requests for products or services that are entirely new to the Organization will go through a very extensive research process to accurately ascertain the associated risk level. Requests for products or services that are known to the Organization will be required to go through only enough research to verify that no significant changes have occurred since the previous acquisition request. Known products can include previously purchased products (e.g., purchasing additional units), and known services can include contracts that are being renewed.

Once the risk level for an acquisition request has been identified, the Organization will develop a list of mitigations tailored to the usage of the specific products and services, which the requester will acknowledge and agree to fulfill before the request will be approved. Mitigations will be determined through the combined efforts of the Acquisition Capability and Risk Mitigation Capability. If the requester fails to acknowledge and agree to fulfill the mitigations, the Organization will not approve the request. The Organization will perform follow-up inspections to ensure that the requester is in compliance with the required mitigations. In addition, because the acquisition process includes considerations as to how the product is used, the Organization also will verify that the acquired product is being used in the approved manner.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Vulnerability Assessment–The Acquisition Capability relies on the Vulnerability Assessment Capability to provide security testing for products to see if they can fit

into the approved products baseline and if not to provide security testing prior to deployment on operational networks.

- Risk Analysis–The Acquisition Capability relies on the Risk Analysis Capability to perform analysis on requested acquisitions to determine the mission impact of the risk they present to the Enterprise.
- Risk Mitigation–The Acquisition Capability relies on the Risk Mitigation Capability to provide mitigation techniques to requesters, which reduces the risk of requested acquisitions to an acceptable level.
- Finance–The Acquisition Capability relies on the Finance Capability to ensure that the Enterprise has appropriately budgeted for IA throughout the acquisition process.
- Operations and Maintenance–The Acquisition Capability relies on the Operations and Maintenance Capability to ensure that acquisition requests have lifecycle plans that include the secure operation and maintenance of the product.
- Decommission–The Acquisition Capability relies on the Decommission Capability to ensure that acquisition requests have lifecycle plans that include the secure decommission of the product.
- IA Policies, Procedures, and Standards–The Acquisition Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards to suppliers and vendors, as necessary.

7.2 Core Interrelationships
The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management–The Acquisition Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Awareness–The Acquisition Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training–The Acquisition Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Acquisition Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Hardware Device Inventory–The Acquisition Capability relies on the Hardware Device Inventory Capability to monitor hardware devices as soon as they are acquired by the Enterprise.
- Software Inventory–The Acquisition Capability relies on the Software Inventory Capability to monitor software assets as soon as they are acquired by the Enterprise.

8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*	
SA-6 *SOFTWARE USAGE RESTRICTIONS*	Control: The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; Enhancement/s: (1) The organization: (a) Prohibits the use of binary or machine executable code from sources with limited or no warranty without accompanying source code; and (b) Provides exceptions to the source code requirement only for compelling mission/operational requirements when no alternative solutions are available and with the express written consent of the authorizing official.
SA-4 *ACQUISITIONS*	Control: The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards: a. Security functional requirements/specifications;

b. Security-related documentation requirements; and
c. Developmental and evaluation-related assurance requirements.
Enhancement/s:
(1) The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.
(2) The organization requires in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls to be employed within the information system, information system components, or information system services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls.
(3) The organization requires software vendors/manufacturers to demonstrate that their software development processes employ state-of-the-practice software and security engineering methods, quality control processes, and validation techniques to minimize flawed or malformed software.
(4) The organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.
(5) The organization requires in acquisition documents, that information system components are delivered in a secure, documented configuration, and that the secure configuration is the default configuration for any software reinstalls or upgrades.
(6) The organization:
(a) Employs only government off-the-shelf (GOTS) or commercial off-the-shelf (COTS) information assurance (IA) and IA-enabled information technology products that composes an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; and

	(b) Ensures that these products have been evaluated and/or validated by the NSA or in accordance with NSA-approved procedures. (7) The organization: (a) Limits the use of commercially provided information technology products to those products that have been successfully evaluated against a validated U.S. Government Protection Profile for a specific technology type, if such a profile exists; and (b) Requires, if no U.S. Government Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, then the cryptographic module is FIPS-validated.
SA-12 *SUPPLY CHAIN PROTECTION*	Control: The organization protects against supply chain threats by employing: [Assignment: organization-defined list of measures to protect against supply chain threats] as part of a comprehensive, defense-in-breadth information security strategy. Enhancement/s: (1) The organization purchases all anticipated information system components and spares in the initial acquisition. (2) The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services. (3) The organization uses trusted shipping and warehousing for information systems, information system components, and information technology products. (4) The organization employs a diverse set of suppliers for information systems, information system components, information technology products, and information system services. (5) The organization employs standard configurations for information systems, information system components, and information technology products. (6) The organization minimizes the time between purchase decisions and delivery of information systems, information system components, and information technology products.

	(7) The organization employs independent analysis and penetration testing against delivered information systems, information system components, and information technology products.
SA-13 *TRUSTWORTHINESS*	Control: The organization requires that the information system meets [Assignment: organization-defined level of trustworthiness].
SA-14 *CRITICAL INFORMATION SYSTEM COMPONENTS*	Control: The organization: a. Determines [Assignment: organization-defined list of critical information system components that require re-implementation]; and b. Re-implements or custom develops such information system components. Enhancement/s: (1) The organization: (a) Identifies information system components for which alternative sourcing is not viable; and (b) Employs [Assignment: organization-defined measures] to ensure that critical security controls for the information system components are not compromised.
SC-18 *MOBILE CODE*	Enhancement/s: (2) The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets [Assignment: organization-defined mobile code requirements].

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Acquisition Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICD 500 Director of National Intelligence, Chief Information Officer, August	Summary: This directive establishes the responsibilities of the Associate Director of National Intelligence/Chief Information Officer (ADNI/CIO). It states all major systems

2008, Unclassified	acquisitions that include the procurement of Enterprise Architecture-related IT items shall adhere to the applicable ADNI/CIO Enterprise Architecture, standards, protocols, and interfaces.
ICD 801 Acquisition, 16 August 2009, Unclassified	Summary: This directive establishes the overarching policy of the Director of National Intelligence (DNI) relevant to the DNI's acquisition authorities and related procurement authorities.
ICPG 801.1 Acquisition, July 2007, Unclassified	Summary: This policy provides guidance on management, processes and plans, program reviews and assessments, and workforce development for acquisitions. It presents the IC acquisition approach, which is to follow the Intelligence Community Acquisition Model (ICAM).
DCID 7/6 Community Acquisition Risk Center, 2 March 2005, Classified	Summary: It is Intelligence Community (IC) policy that the IC shall use a common threat, vulnerability, and risk assessment methodology for acquisitions to protect, to the maximum extent feasible, sources and methods from foreign exploitation.
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DoDD 4630.05 Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 5 May 2004, 23 April 2007, Unclassified	Summary: This directive established policy: It is Department of Defense (DoD) policy that: 4.1. IT and National Security Systems (NSS) employed by U.S. Forces shall, where required (based on capability context), interoperate with existing and planned, systems and equipment, of joint, combined and coalition forces and with other U.S. Government departments and agencies, as appropriate. The DoD shall achieve and maintain decision superiority for the warfighter and decision-maker by developing, acquiring, procuring, maintaining, and

	leveraging interoperable and supportable IT and NSS. 4.3. IT and NSS interoperability and supportability needs shall be derived using Joint Operating Concepts, Joint Functional Concepts, and associated integrated architectures and shall be updated as necessary throughout the system's life. For IT and NSS supporting DoD business areas and domains, the Global Information Grid (GIG) Architecture shall be used to determine interoperability and capability needs. IT and NSS interoperability and supportability needs, for a given capability, shall be identified through the following: 4.3.1. The Defense Acquisition System…
DoDI 4630.8 Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 30 June 2004, Unclassified	Summary: It is DoD policy that: 4.1. IT and NSS employed by U.S. Forces shall, where required (based on capability context), interoperate with existing and planned, systems and equipment, of joint, combined and coalition forces and with other U.S. Government departments and agencies, as appropriate. The DoD shall achieve and maintain decision superiority for the warfighter and decision-maker by developing, acquiring, procuring, maintaining, and leveraging interoperable and supportable IT and NSS.
DoDD 5000.01 The Defense Acquisition System, 12 May 2003, Certified current as of 20 November 2007, Unclassified	Summary: This directive provides management principles and mandatory policies and procedures for managing all acquisition programs.
DoDI 5000.02 Operation of the Defense Acquisition System, 8 December 2008, Unclassified	Summary: This instruction "establishes a simplified and flexible management framework for translating capability needs and technology opportunities, based on approved capability needs, into stable, affordable, and well-managed acquisition programs that include weapon systems, services, and automated information systems (AISs)."
DoDD 5144.1 Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, 2 May	Summary: This directive establishes responsibilities for the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)): 3.3.9. Design and implement, in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), the

2005, Unclassified	Under Secretary of Defense (Comptroller)/DoD Chief Financial Officer (USD(C)/CFO), the Under Secretary of Defense for Intelligence (USD(I)), and the Chairman of the Joint Chiefs of Staff, a process for maximizing the value and assessing and managing the risks of DoD IT acquisitions, including NSS acquisitions, as applicable.
DoDD 8000.01 Management of DoD Information Enterprise, 10 February 2009, Unclassified	Summary: This directive establishes policy that all aspects of the DoD Information Enterprise, including the GIG infrastructure and Enterprise services and solutions, shall be planned, designed, developed, configured, acquired, managed, operated, and protected to achieve a DoD net-centric environment. The DoD Enterprise Architecture shall be maintained and applied to guide investment portfolio strategies and decisions to establish and enforce standards and guide security and IA requirements across the DoD. It also sets policy that requires the review of all IT investments for compliance with these architectures and IT standards.
DoDI 8580.1, Information Assurance (IA) in the Defense Acquisition System, 9 July 2004, Unclassified	Summary: This directive established policy: It is DoD policy that: 4.1. IA shall be implemented in all system and services acquisitions at levels appropriate to the system characteristics and requirements throughout the entire lifecycle of the acquisition. 4.2. All acquisitions of mission-critical or mission-essential IT systems, as defined in reference (e), shall have an adequate and appropriate Acquisition IA Strategy that shall be reviewed prior to all acquisition milestone decisions, program decision reviews, and acquisition contract awards.
DTM 09-019 Policy Guidance for Foreign Ownership, Control, or Influence (FOCI), 2 September 2009, Updated 8 June 2010, Unclassified	Summary: This directive-type memorandum (DTM) provides guidance for and establishes procedures concerning the initial or continued facility clearance (FCL) eligibility of U.S. companies with foreign involvement, provides criteria for determining whether U.S. companies are under FOCI, prescribes responsibilities in FOCI matters, and outlines security measures that may be considered to mitigate the effects of FOCI to an acceptable level.

Committee for National Security Systems (CNSS)	
NTISSP 11 Fact Sheet for the National Information Assurance Acquisition Policy, July 2003, Classified	Summary: This document establishes policy: IA shall be considered as a requirement for all systems used to enter, process, store, display, or transmit national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated government off-the-shelf (GOTS) or commercial off-the-shelf (COTS) IA and IA-enabled IT products.
Other Federal (OMB, NIST, …)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	

Acquisition Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
NIST SP 800-23, Guidelines to Federal	Summary: This guideline advises departments and agencies to develop policies for the procurement and use of evaluated

Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, August 2000, Unclassified	products as applicable. It further recommends agencies should give substantial consideration in IT procurement and deployment for IT products that have been evaluated and tested by independent accredited labs against appropriate security specifications.
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, …)	
Nothing found	

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Number of acquisitions–Each acquisition requires the use of resources. The more acquisitions an Enterprise has the more resources that will be used.

2. Research requirements–Each acquisition that is not already known by the Enterprise requires research to ascertain its risk level. The Enterprise may use external contracts for information gathering, including the collection of open source information.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Acquisition Capability.

- The Enterprise mitigates security risks associated with acquisitions spanning all purchases, including hardware, software, services (e.g., people and maintenance), and products not related to IT.
- The Enterprise shall determine the security risk level (e.g., low, medium, or high) associated with each proposed acquisition.
- The Enterprise shall consider the supplier and how the product is going to be used in the Enterprise environment.
- Suppliers shall be vetted to ensure that they meet the Enterprise assurance requirements.
- If the supplier is a value-added reseller, the Enterprise shall determine the value being added to the product and verify that the value-added reseller is not implementing anything malicious or anything that may degrade the product's ability to effectively implement security functions.
- All products shall be handled by original suppliers that produce it until the purchasing Enterprise receives it.
- The Enterprise processes shall conform to security practices as established by the Enterprise's policy and standards.
- The Enterprise shall take into account the policies that govern where the product will be implemented when implementing consistent supply chain risk management.
- When possible, the Enterprise shall require that suppliers follow the IA policies, procedures, and standards set forth by the Enterprise to reduce the level of risk associated with the supplier and its products.
- The Enterprise shall evaluate the background of personnel performing development activities and business processes on products.
- The Enterprise shall require that certain products or services be worked on only by individuals who hold a certain security clearance.

- All acquisitions shall have an associated mitigation plan including a set of mitigation steps that must be taken to reduce to an acceptable level the risk associated with the proposed acquisition.
- Free and open source software like any other product shall be accounted for by the Enterprise.
- A product's risk assessment report shall be shared with the appropriate IA management personnel for each acquisition that is proposed.
- Acquisitions shall be approved prior to procurement for acquisition requests involving removable media or requests that require the Enterprise to develop a test plan.
- The Enterprise shall maintain system and network documentation in accordance with Enterprise policy and procurement updates.
- External contracts that include IA shall be in compliance with IA standards as a required performance element.
- All commercial contracts and COTS products shall be vetted and reviewed prior to procurement by the Enterprise.
- All COTS products shall be further tested by the Enterprise for unexpected behavior and security, prior to being placed in the operational environment.
- When GOTS products or service providers can implement IA within the contract, the Enterprise shall include provisions for the foreign procurement of product components and the development of anonymity plans.
- All products shall be preconfigured for security to ensure that acquisition security cannot be circumvented.
- The Acquisition Capability shall establish a comprehensive information security strategy to mitigate risks from the supply chain.
- The Enterprise shall know the provenance of the IT products and services provided by suppliers.
- The Enterprise shall require transparency in the product design and development processes employed by suppliers.
- The Enterprise shall be balanced against federal acquisition regulations, which require simplified acquisition procedures.
- The Enterprise shall minimize the time between decisions to purchase products or services and the actual delivery date of the products or services.
- The Enterprise shall use standard configurations of products and systems to reduce the probability of malicious code insertion.
- The Enterprise shall protect purchasing information, including the buyer's identity.

- The Enterprise shall ensure approved distribution processes for products and services. This may be more difficult to achieve with COTS products than with GOTS products because the development of GOTS products can usually be more controlled.
- The Enterprise shall use products that come with manufacturer-supplied unique identifiers, when possible (i.e., serial numbers).
- The Enterprise shall use products that have been through an appropriate level of testing and certification, where applicable, such that they are approved for use in the Enterprise.
- The Enterprise shall define a baseline of products that can be used within the Enterprise. Acquisitions outside of the designated baseline shall be considered on a case-by-case basis, with final approval from the appropriate Enterprise authority.